Blueshift RESEARCH REPORT

Seth Agulnick, sa@blueshiftideas.com

Elastic Faces Tall Task to Set Itself Apart from Amazon, Others

Companies: AMZN, CSCO, DDOG, DT, ESTC, GOOG/GOOGL, IBM, MDB, MSFT, NEWR, ORCL, SPLK, SUMO

August 5, 2021

Report Type: ☐ Initial Coverage ☑ Previously Covered ☑ Full Report ☐ Update Rating: 2/5

Research Question:

Has Elastic found the right formula to stand out from the competition in search, security, and observability?

Summary of Findings

- Elastic N.V.'s (ESTC) underlying platform is broadly appealing for its variety of uses across enterprise search, security, and monitoring but the value of Elastic's paid features are less clear, making the company increasingly vulnerable to Amazon.com Inc.'s (AMZN) OpenSearch, a free version of Elastic's core product, according to 11 interviews with users, channel partners, and industry specialists.
- Amazon's version of Elasticsearch is an easy choice for many Amazon Web Services (AWS) cloud customers, three sources said, largely because of its easy integration with other Amazon services. One source suggested it would be "game over" for Elastic if Amazon offers a fully managed version of its forked Elasticsearch service.
- Elastic's recent licensing model change, aimed at preventing Amazon from reselling its product, is not likely to help much, four sources said. One called Elastic's IP a "hollow shell" and another said the change could steer some users and developers to Amazon, since its product is now the only fully open-source version.
- Elastic's unified backend architecture is not a big advantage, four sources said, nor is it spurring adoption of other Elastic solutions beyond search, such as security and observability. One source with a competing vendor said companies need to run multiple clusters for logs, search, and application performance monitoring (APM), so there is little advantage to Elastic's single-stack technology compared to using multiple vendors for observability.
- Source feedback was more negative than in Blueshift Research's Feb. 6, 2020, report, especially around the threat from Amazon. One repeat source who was bullish on Elastic last year but more negative this time said the improvement in Amazon's version is a key reason for his change in sentiment. The source, an enterprise search consultant, said almost all of his clients are using the Amazon version in AWS and none are using Elastic Cloud, a shift from 18 months ago.
- Elastic users were generally complimentary about the underlying platform, praising its ability to handle a wide variety of data types, its improving security suite, its enterprise-level support, and the addition of machine learning (ML) features. However, only one is paying for an Elastic license; two others are using the free version on premise and one is using the Amazon version in AWS.

Silo Summaries

1) Elastic Users

Only one of five sources in this silo is currently paying for an Elastic license. Three others are using the free version, including one using Amazon's product within AWS. **Elastic's platform has some appealing attributes, such as its ability to handle a wide variety of data types, its active user community, and some new machine learning features**. The support offered by Elastic to paying subscribers is a key benefit of a subscription. However, **Amazon could severely damage Elastic's prospects with a fully managed version of its Elasticsearch clone**. Elastic's recent license model change is not likely to have much impact. Elastic's unified architecture is helpful in managing the platform but is not an important advantage.

2) Industry Specialists

The four sources in this silo were generally negative about the value of Elastic's paid features and its ability to stand out from competitors. **Elastic's underlying platform is easy to get up and running, but its paid version is not very compelling and Elastic is having a hard time differentiating itself from Amazon and others.** Amazon's product has made significant strides with features that Elastic charges for, such as security and user authentication. **Elastic's new licensing model will not alter the competitive dynamics and has sparked some distrust of Elastic among developers devoted to the open-source model.** Elastic's single-stack technology is not a differentiator.

3) Elastic Partners

Elastic offers a more agile way to approach logging and security incidents management than other enterprise platforms. Elastic meets expectations for cost savings as long as companies have the human resources talent to customize the platform for their specific use cases. To grow in the face of pressure from Amazon's competing product, Elastic will have to find ways to keep adding value on top of the open-source product.

4) Competitor Partners

Splunk has more appeal than Elastic in enterprises for which time, security, and out-of-the-box features are the main concern, rather than upfront cost. Security tools are not converging with APM, infrastructure monitoring, and logging. Security teams are usually separate from standard IT functions in an organization and use their own tools.

	Elastic's Differentiation from Competitors	Elastic's Security Tools	Elastic's Observability Suite
Elastic Users	→	↓	→
Industry Specialists	↓	→	↓
Elastic Partners	↑	↑	→
Competitor Partners	→	NA	↓

Background

Elastic—a developer of software for enterprise search, IT security, and network observability—continued its march toward $1 billion in annual revenues with a strong end to its fiscal 2021. Its fourth-quarter (Q4) revenues were up 44% to $178 million, including 77% growth in Elastic Cloud revenues, while full-year sales surged 42% to $608.5 million. Elastic finished the fiscal year with more than 15,000 subscribers, including over 730 with annual contract values of more than $100,000. Its net retention rate, which has been one of the company's standout metrics, did slip below 130% in the quarter. Executives have forecast about 33% revenue growth for the current quarter and 29% for the full fiscal year. The company says it is on track to reach $1 billion in annual revenues in fiscal year 2023.

Elastic has been pushing to expand the appeal of its core search software to enterprises. A company-sponsored survey suggested that the COVID-19 pandemic and resulting increase in employees working from home was making business search more critical than ever. About 60% of respondents working remotely said they spend more time looking for documents than they do replying to messages or emails. In a move aimed at enterprises, Elastic recently launched its "searchable snapshots," which allow companies to search data that is housed in lower-cost "cold" or "frozen" storage. Executives said the feature is especially appealing to large companies that hold on to vast troves of data. Elastic said one of the world's largest telecommunications companies recently upgraded to an enterprise subscription from the free, basic tier in order to take advantage of searchable snapshots and the associated frozen data tier.

One of the key issues for Elastic is that the vast majority of its customers use a free version of its mostly open-source platform. Others use a free version with the same underlying code offered by Amazon to its AWS cloud customers, called OpenSearch. While its relatively low subscriber count gives Elastic much room for growth by converting users to a paid subscription, it also leaves it competing with free options that are good enough for many companies. Earlier this year, Elastic announced a change to its licensing that was largely an effort to fend off Amazon. In announcing the adjustment, Elastic's CEO said AWS has "been doing things that we think are just not OK since 2015 and it has only gotten worse. If we don't stand up to them now, as a successful company and leader in the market, who will?" The new licensing system is aimed at keeping companies like Amazon from providing Elasticsearch as a service without collaborating with Elastic and making all of the hosting cloud's infrastructure open source.

In addition to Amazon, Elastic competes in various segments with Microsoft Corp. (MSFT), Alphabet Inc.'s Google (GOOG/GOOGL), IBM Corp. (IBM), Oracle Corp. (ORCL), Datadog Inc. (DDOG), Splunk Inc. (SPLK), and others. In April, Elastic moved into the "visionary" segment of Gartner's Magic Quadrant for Application Performance Monitoring, a market led by Dynatrace Inc. (DT), Cisco Systems Inc. (CSCO), and New Relic Inc. (NEWR). The company was praised for its scalability and its flexibility in deployment models and pricing. The report noted, however, that Elastic's stack is complex and "often requires significant manual tuning to support large volumes of data storage." Gartner also named Elastic's enterprise search product a "challenger" in the Insight Engines segment, where the leaders include Mindbreeze, Sinequa, and Coveo. Gartner gave Elastic credit for being innovative but said, "missing is a broader vision for search."

Security products account for only about 20% of Elastic's business but represent its fastest growing segment. The company recently added malware and ransomware defense mechanisms to its product suite as it continues to integrate its $234 million acquisition of Endgame. Elastic has also become a key player in the evolving observability market, which combines

tools around data logs, metrics, and application performance monitoring. Elastic recently unveiled an expanded integration with Microsoft that allows customers to onboard logs and metrics for their Azure services directly in Azure to Elastic's observability solution. Elastic believes it has a winning formula in observability because of the combination of its various tools in a single stack architecture.

Blueshift's 2020 report suggested use of Elastic's solutions should continue to grow because the company offers a fast, powerful stack of enterprise search and monitoring technologies. Sources said the underlying software's ease of use, an active developer community, and frequent updates have combined to make Elasticsearch and its related tools the platform of choice for a wide range of uses and industries. Sources did caution that Elastic faces some challenges in getting users to pay for licenses rather than choose the free, open-source version available from both Elastic and Amazon. Blueshift's September 10, 2020, report on the observability market noted that the segment is highly competitive and that customers often use multiple vendors to meet their needs. New Relic, Dynatrace, and Cisco were cited as sector leaders.

Current Research

Blueshift Research assessed Elastic's competitive positioning in its key markets. We employed our pattern mining approach to establish five independent silos, comprising 11 primary sources (including four repeat sources from various reports) and one secondary source focused on the license dispute between Amazon and Elastic. Interviews were conducted July 19–30.

1) Elastic users (5)
2) Industry specialists (4)
3) Elastic partners (1)
4) Competitor partners (1)
5) Secondary sources (1)

Next Steps

Blueshift Research will continue following the evolution of Amazon's forked Elasticsearch offering, including its impact on Elastic and its developer community.

Silos

1) Elastic Users

Only one of five sources in this silo is currently paying for an Elastic license, although a second–a freelance Elastic expert—said a paid subscription has value. Three others are using the free version, including one using Amazon's product within AWS. All five sources said Elastic's platform has some appealing attributes, such as its ability to handle a wide variety of data types, its active user community, and some new machine learning features. The support offered by Elastic to paying subscribers is a key benefit of subscription, according to one source. However, Amazon could severely damage Elastic's prospects with a fully managed version of its Elasticsearch clone, one source said. Such a product would be simple to deploy and have the advantage of easy integration with other AWS services, he said. Elastic's recent license model change, aimed at preventing Amazon from reselling Elasticsearch, is not likely to have much impact, according to two sources. Within enterprise search, one source said he does not believe any competitors can match Elastic's functionality and scale, but two others mentioned Solr and MIT's InfluxDB as having some advantages over Elastic. One said Elastic's focus in areas beyond search has left its core product weakened. Within security, Elastic cannot match vendors offering real-time data aggregation because of its search-based approach and its customers are going to want specialized solutions rather than Elastic's broad-based platform, according to one source. Another, however, said Elastic's security suite is relatively new and eventually will be among the best available, especially with the addition of event query language (EQL), stemming from its acquisition of Endgame. In observability, Elastic has some compelling advantages, two sources said, including its community and its ability to integrate into many enterprise components. One source said his company is having some scaling issues with Elastic. Observability is becoming so critical that big players like Amazon and Google are building out their capabilities and Elastic is unlikely to be able to match their solutions, one source said. Elastic's unified architecture is helpful in managing the platform but is not an important advantage, one source said.

Key Silo Findings

Deploying Elastic

- 1 of 5 is using the paid version of Elastic with a platinum license, hosted on AWS. 2 are self-managing the free version of Elastic on premise. 1 is using Amazon's free version on AWS. 1 is a freelancer who has worked with multiple versions.
  - 1 of the users of the free version said his company will consider switching to a paid subscription because it wants to resell a customized Elastic product, which it can no longer do with Elastic's recent license change.
  - 1 other user of the free version said certain features like machine learning could cause him to push his company to upgrade to a paid subscription.
- 3 said Elastic's machine learning capabilities are an appealing feature, while 1 other said ML is an opportunity for Elastic that it has not fully explored outside of security.
- 1 said deploying Elastic's platform in the Elastic Cloud is a great setup because it is fully managed. 1 other said he tried Elastic Cloud and found its performance lacking because of its focus on resiliency.
  - 1 who was negative on Elastic Cloud said the value it adds is in areas like AI that companies can get from their security tools.
- 1 said Amazon represents an existential threat to Elastic if it decides to offer a fully managed version of Elasticsearch with its own proprietary customizations.
  - Amazon appears to be moving in that direction, with some forking from the open-source Elasticsearch, addressing some of the modules in the paid version from Elastic.
  - Such a fully managed version will be well known quickly, easy to run, and simple to integrate with other AWS services.
  - The improvements Elastic has made to Lucene, the backbone of Elasticsearch, are not anything Amazon and others cannot replicate.
  - The dispute between Amazon and Elastic is similar to the fight Amazon had with MongoDB Inc. (MDB) before Amazon built a clone, DocumentDB.
- 1 who is using the free version of Elastic on premise said switching to Amazon's version in the cloud might end up adding costs because of the storage required.
- 1 said Amazon's version of Elasticsearch pales in comparison to paid versions of Elastic, especially because of key security features in the latter.
- 1 said Elastic's recent license model change will do nothing to hold off the threat from Amazon. 1 other said some users may be drawn to Amazon's version as a result of the license change because it is now the only true open-source version.
- 1 using the paid version of Elastic said he expects his company's spending on the product to increase because it is expanding its observability, machine learning, and security capacity and use cases. 1 other said clients often increase spending on Elastic over time because of free trials that give them a taste of useful features.
- 2 said Elastic's active user community is a key advantage to using the platform.
  - 1 said Elastic's brand name is very strong in the developer community.
- 2 said Elastic's platform has been improving, especially around its Kibana tools.
- 3 praised Elastic's platform for its ability to ingest and process disparate types of data.
- 1 said the combination of MIT's InfluxDB with Grafana provides better performance than Elasticsearch and Kibana.
- 1 said Elastic requires a lot of computing resources.
- 1 said aggregation with Elastic, such as transactions per second, can be extremely slow and sometimes fails over longer durations.
- 1 said he would like to see Elastic extend hosting to other cloud providers, as Google and AWS can be very expensive.
- 1 said Elastic should add multi-tenancy capabilities to allow easy segregation of multiple customers' data sets.
- 1 said initial deployment of Elastic has gotten significantly easier in the last two years with the Elastic Agent.

Enterprise Search

- 1 said he is not aware of any vendor that can replicate Elastic's enterprise search capabilities with the same functionalities and scale.
- 1 said Elastic's search product has become weaker because the company has been focusing on other areas.
- 1 said Solr is integrated in many content management systems and is growing as a challenger to Elastic in search.
  - Solr is more difficult to operate, however.

- 2 said Elastic's integration with Kibana is an important differentiator.
  - 1 said Solr and InfluxDB can match Elastic's capabilities in search but the latter's integration with Kibana provides key capabilities that help with triaging issues and monitoring.
    - Solr and InfluxDB could be a bigger threat to Elastic, with better visualizations for backend data.
  - 1 said building dashboards with Kibana offers more power than what is available with Amazon's version.

Security

- 1 is using Splunk for security and 1 other is using Exabeam.
- 1 said Elastic's search-based approach to security will never be as quick as products that perform real-time aggregation for detecting problems.
- 1 said specialized security monitoring software is preferable to Elastic's broader approach.
- 1 said Elastic's acquisition of Endgame has added event language query to its security platform, a huge advance for correlating multiple events over time.
  - The Elastic user community is extremely excited over the addition of EQL.
- 1 said Elastic's security suite offers wider visibility than competing products, making it easier to ingest multiple data sources and easier to work with data.
- 1 listed Azure Sentinel, IBM, and Splunk as Elastic's key competitors in security.
  - IBM has a top offering, while Splunk is losing share.
- 1 said Elastic's security suite will take some time to mature, as many of its key features have only been introduced in the last year or so.

Observability

- 1 said his firm is using most of Elastic's observability tools, such as APM, logging, and metrics—but not security.
  - Elastic replaced Splunk in his company because the latter's consumption-based model was too expensive.
- 1 said Elastic's advantage over competing vendors is its open-source community, while 1 other said its ability to integrate into many components of an enterprise helps it stand out.
- 1 said Elastic is easy to set up and get started with but his company is having scaling issues, as Elastic requires a lot of hardware.
- 1 said he does not think the different pillars of observability are converging into a single product because rapidly evolving security threats require dedicated and specialized tools.
- 1 said improvements in Amazon's dashboarding mean his company is likely to switch to AWS completely for observability rather than continue to send data from Amazon's CloudWatch to Elastic.
- 1 said cloud vendors like Amazon and Google are developing their observability and search capabilities because of how important those functions have become and their solutions are likely to be better than anything Elastic or similar vendors can offer.
- 1 said Elastic's unified architecture does offer some management advantages but is not a key selling point.

1) Solution architect for a national TV broadcaster in Asia Pacific

Amazon is an enormous threat to Elastic's future if it decides to offer a fully managed version of Elasticsearch with its forked product that adds new features. Within enterprise search, Elastic seems to have lost focus as it has expanded to new segments. Solr is a growing challenger in search, especially because it is already integrated into many content management systems. In security, most companies are going to want specialized solutions rather than a broader platform like Elastic, whose searched-based approach is not as fast or comprehensive as other solutions. The Elastic Cloud has been built for resiliency but its architecture hurts performance.

Deploying Elastic

- "I've used Elastic's tools in all three [segments]: search, security, and observability."
- "We currently use [Elastic] for logging, so we use Kibana quite heavily on the main infrastructure side for AWS. Low-level log analytics are probably our main [use for Elastic]."
- "We also have New Relic, though, for high-level [analytics]—more application-level stuff. But we may well phase that out and just move to more generic [observability tools] within the AWS environment, like CloudWatch."
- "There's a few edge cases [where I've also used Elastic]. There's a big data angle as well, which is very much a niche thing that some people use Elastic for. I've used Elastic for that purpose in the past—data exploration, basically."

- "We do use Elastic for [data exploration] in the content space to some degree, to explore archive stuff, so it's useful for that in terms of story research. But that's very niche because it's only for media entities. But, in terms of our archives of video, Elastic is not really search, but more discovery of relationships between things because it can be used for inference."
- "I think there's a kind of ML angle that I don't think [Elastic] has fully explored. ML is more directed to the security space but there are other uses for the ML functions."
- "We have used paid versions [of Elastic]—its cloud version—[but] we now use the AWS SaaS [software as a service] version of Elastic. We were at one point briefly using Elastic Cloud, and now we're using AWS Cloud. We're still [also] using Mongo Cloud but we're not using Elastic Cloud [because] it didn't really work well. There are some major problems with the way [Elastic] architected that for use for search, particularly. It's not really ideal the way they've set it up."
- "[Elastic Cloud] has been designed to be conservatively resilient so, in terms of the performance you get out of it, you effectively pay double. You pay less if you're a really large set-up but most [enterprises] are paying double [because Elastic] doesn't give you access to the query performance of you having a lot of nodes; they use those as backups. So you're kind of paying for backups you can't use."
- "The 'hot standby' approach Elastic Cloud chose to use is more than twice as expensive than the AWS version for the same day-to-day capacity but loses no capacity at all if a failure occurs. It's a tradeoff that makes sense for a smaller SaaS vendor to make customers happier but poorer."
- "The Amazon set-up lets you use all the capacity—you over-capacity it but you still get it as a burst. And the thing is, for a media organization like ours, we really smash our search engines during, say, the World Cup, and we actually use search to drive the navigation, as a lot of people do these days."
- "Our whole on-demand website is driven by search; it's searching continuously, so that even when it looks like you're navigating, you're actually searching, which is very common. Amazon does this, too. The problem is that the search traffic is enormous. The fundamental problem with [Elastic's] cloud product is that you pay a lot of money for the capacity you get, and that's just a decision they made to make it as resilient as possible, to make switchovers really transparent [so that] when a failure occurs within Elastic Cloud, you basically don't notice because there's a whole backup there. The benefit is you don't see a difference."
- "The downside is you're paying twice. Most media organizations, because we have to handle high bursts, we don't want that; we want to be able to use all of our traffic, all of our ability. We don't want to fail completely but we don't really want to pay [for the way Elastic has set up its cloud]. We're on a fixed budget and most organizations are the same; we're trying to do cost containment."
- "To handle those bursts, you can't scale something like Elasticsearch instantly. It takes a reasonable amount of time—maybe 10 minutes—to stand up the backup. That's why [Elastic] has done what they've done; the backup's always there, so if it fails, the backup kicks in and you don't notice it, which is great from a customer care point of view in terms of them not having to get people up in the middle of the night if something goes wrong. So it's very good for keeping their staffing down, in terms of key technical operations roles."
- "The things you get [from Elastic Cloud], the value add, it depends on what kind of company you are and how technical you are. I think there are some enterprises, say, in marketing, that want the capabilities that Elastic gives you with the plug-in modules that come bundled with the cloud. But the problem is that some of those things are in areas like pattern recognition. It's an AI add-on that you probably would get, as we did, from our security product."
- "Elastic is now very popular in the AWS environment and AWS is all-in on the cloud search stuff. The existential threat to Elastic is, because they started out as open source, their value-adds are pretty specific—the ones you get with the cloud service."
- "Every time it comes up, we look at Elastic Cloud and figure out if it's going to make sense. There would be a lot of people out there like me who will always consider Elastic. I think the brand is pretty strong; a lot of developers know what Elasticsearch is."
- "But the threat to [Elastic] is the obvious one, and that's AWS, which is a massive competitor. If they introduce a [fully managed search product], a lot of people are going to know about it very quickly and will be prepared to give it

> **The threat to [Elastic] is the obvious one, and that's AWS, which is a massive competitor. If they introduce a [fully managed search product], a lot of people are going to know about it very quickly and will be prepared to give it a go.**
>
> *Solution architect for a national TV broadcaster in Asia Pacific*

a go. Amazon is really good at making sure people know the name of their service, which will be something obvious like, 'Amazon Cloud Search.'"

- "I can't guarantee that Amazon goes all-in on having their own [search tools] but, if it happens, it's going to happen pretty suddenly. The question will be, what value-add will Elastic Cloud add or [will its] license add? And the answer is, not a lot, because the components that are available on Amazon that you can integrate pretty easily around ML or whatever would wipe the floor."
- "Because it will probably be a completely braindead implementation, where it's concierged. You'll just pump data into it and you just pay by the amount of data you put in and you pay by the queries you do. That model will be so attractive."
- "Elastic Cloud is not a bad product but it's got some strange scaling anomalies and other things that people notice when they start using it—some things about it that [Elastic] should have fixed up a long time ago—and which AWS has [addressed]."
- "One example, which they may have fixed now, is that you could only use two of [Elastic Cloud's] availability zones. [Our country] has had three of these data centers in AWS for a really long time but you could only use two [with Elastic], whereas Amazon let you use three, which is better for resilience and cost because, if one fails, you only lose a third of your capacity, not half."
- "There are still a bunch of things about Elastic Cloud that, last time we looked at it, [weren't optimal] and the thought was, 'This is just too expensive.' So we did go through that whole exercise of looking at whether we'd use it again. We tried it, we paid for it for a while, and we decided no, it's costing us more money and it's not that much harder to run it ourselves on AWS using [AWS'] semi-managed service."

Enterprise Search

- "Elastic has a good community side to them, particularly for observability and to some extent security, where they have a fairly big mindshare. But search? No. On the community side for search, they're hopeless. You're better off dealing with the Solr people because they care about search, whereas I'm really not convinced Elastic cares very much about search. If you go to their conferences, there's very little about search because I don't think that's why [the software] was done in the first place."
- "What I like about Elastic is that it's easier to operate than Solr. Solr is hard to run and requires specialist people who know what they're doing. There is no real useful cloud version of it and so, in our case, if it's inside a managed CMS [content management system], it's OK, because someone else is running it for you and you don't care. But if you're having to run it, as we do at the moment for some purposes, it's hard work. Our ops team hates [Solr] and they like Elastic. It's easier to run and a lot more resilient when things fail."
- "I'm a fan of Elastic, to be clear, but I'm also aware of this swirling tension when it comes to search, which is that a lot of the CMS vendors use Solr. Our main vendor for our CMS, they use Solr, and historically quite a lot of CMSs we've had have used Solr. Drupal uses Solr, for example."
- "Solr seems to be making a bit of a push to become commercial again. … We went through a phase where we were using Elastic more but we're now going back to Solr, mainly because our CMS vendor, which is also sort of our API [application programming interface] vendor on the content side now … will be using Solr because that's what's built in at this stage."
- "I think Solr has been resuscitated to a degree. That project was in decline but they seem now to be pushing back into the search space. They've always been stronger on the search side because the people who work on the Solr project are more search engineers, in terms of using it for the purposes of content discovery—both editorially, where you're looking for stuff in your archive, and from a customer point of view, which is doing searches on your site."
- "Elastic didn't really put any focus on the search side for a long time. They seem to have almost weakened that because the log [observability] thing became so huge for them; they seem to have lost focus on search."
- "I would guess that the next move from AWS will be a fully managed version of Elastic, which doesn't exist at the moment. That's the threat. And they'll fork—they'll start adding features to their version that don't exist already [in Elastic's version]."
- "This has already started happening. If you look very carefully at the service catalog for AWS Elasticsearch, they've addressed some of the modules that you get from the paid version from Elastic. This is a guess, but what I suspect is that you're going to see a fully managed version that will be more like Aurora; it will be a fully managed [offering]."
- "The [OpenSearch] fork is not the 'whole way' yet—the SaaS ones hide nodes and scale automatically for storage and performance but that is probably the next step based on Aurora."
- "[Elastic's licensing model change] won't head off the threat from AWS. It's a fail because there's no IP there. It's a hollow shell. It's the same with Mongo. It's not going to work, I'm afraid. [The backbone of Elasticsearch], Lucene,

which is really old—it's been around a long time and is literally an implementation of an area of academic research—Elastic made that more scalable, easier to scale up, and usable for observability but, really, there's nothing they've done that somebody else, particularly Amazon, can't do."

- "The benefit of Elastic is that fairly undertrained people could just stand it up and use it and it would probably run for a year without any problems. Generally speaking, it's easy to run. But if Amazon comes in with a fully managed [version], it's game over, because those services on Amazon are just so well run—not just in search, but in general."
- "Mongo got into a fight with AWS because Mongo didn't like where things were going with Amazon. They realized they were getting cut out of making any money from their product. Amazon then built a clone, effectively, which is DocumentDB. And [the relevance for Elastic] is that Amazon can do the same with Lucene; [AWS] has really good engineers. Solr is out there and basically open source and most of the stack for Elastic is open source, as well. And Amazon can do a hard fork, which is where things are headed, one suspects."
- "There will be a new version of Amazon search. I'm aware of this hard fork that's occurring, where Amazon just wants to rule the world and they don't make any pretense about it. Their approach is to give customers what they want and they're laser focused about it. I think that's the threat to Elastic."
- "Amazon has already had a search engine, which was their commerce search that they pivoted into for AWS. We've looked into Amazon's current search platform and it's rubbish; it's easy to use but it's not very good in terms of a search engine."
- "What one suspects is that a Lucene-type [solution] is coming [from Amazon], given that they've got all the plumbing. … The underlying tensions [between Amazon and Elastic] are there because there is this seismic shift occurring where Amazon—which is really good at the underlying technology that makes Elasticsearch work—is probably going to shaft Elastic, as they did Mongo. That's the deeper thing that's going on, that architects like me [can see coming]. It's this same pattern of tension between Elastic and Amazon that occurred between Mongo and Amazon."
- "There are a lot of competitors in search. There are a heap of enterprise ecommerce search products if you look in the Gartner square."

> **The benefit of Elastic is that fairly undertrained people could just stand it up and use it and it would probably run for a year without any problems. Generally speaking, it's easy to run. But if Amazon comes in with a fully managed [version], it's game over, because those services on Amazon are just so well run.**
>
> *Solution architect for a national TV broadcaster in Asia Pacific*

Security

- "We recently evaluated [Elastic] for security monitoring but we ended up going with Exabeam … which is Gartner top quarter for security management, for SIEM [security information and event management]. It's the top one, the very best. It's both feature rich and rapidly evolving, and very focused just on security."
- "The trouble, I think, with Elastic is that they've diluted themselves a little bit, because they had this operational monitoring vs. security monitoring thing, whereas [Exabeam] is very specialized in security monitoring. It's more or less all they do."
- "One of the problems with Elastic is everything's based on searches, so it's never going to be as quick as a product that's doing real-time aggregation for noticing issues. It basically has to search continuously to figure out whether there's a problem."
- "I'm not the security manager but I'm on the architecture review board, so I'm aware of why we went with a very specialized product instead of using Elastic, which we've already got. We could have upgraded, effectively, or added Elastic Cloud as a side thing off our main login to get all this to work, but we decided not to go that way."
- "In the security space, Elastic has a ton of really hardcore competitors, including the one we selected. We chose Exabeam because our security manager wanted the gold-plated solution and I don't think he's wrong about that. Like a lot of large, public entities, we do get attacked in pretty serious ways."
- "Exabeam is more expensive but it depends on the hierarchy in your infrastructure. We don't pump everything to the security [application]. We send as much as we can but there's this cost management thing you have to do with products like that because they cost you per record, effectively."
- "Exabeam is more expensive than Elastic but it's better because it's fully real time, which is something Elastic is not. [Elastic] is running batches every so often—quickly—to look for problems, vs. Exabeam, which is looking for patterns, continually, in real time. Splunk does that as well; it's continually aggregating in real time and is always up to date."

- "Long term, Exabeam also has some challenges in that eventually you want all of that [security data] in the cloud. We currently have enough on-prem stuff still that Exabeam makes sense, as a lot of organizations do."

Observability

- "No [I don't see evidence of a convergence between APM, infrastructure monitoring, logging, and SIEM]. I think it's going the other way."
- "Exabeam is a good pointer to this. In the security space, [Elastic's security offering] was kind of piggy-backed onto observability and they are close to the same thing. But I think security threats are evolving so rapidly that I'm not sure something generic makes a lot of sense. I think what's happening is that it's becoming more specialized in the security space and my gut feeling is that general vendors [like Elastic] are going to struggle in the space."
- "The reason we use Elastic for monitoring is kind of interesting. For its capability—I've always found this for Kibana—it has some limitations but it's pretty cheap for what it does. Splunk is expensive—very, very expensive. [Splunk] has gotten a bit cheaper over time, and you can obviously haggle with them, but the issue that Splunk has is the way [their architecture is set up] is quite expensive in compute, so they have to have a lot of compute all the time, which they have to charge for. Elastic is about half the cost."
- "If you want to build dashboards, Kibana [is better than AWS tools] because it gives you slightly more power and it's why we're still using [Elastic]. But it's a tension. I think, at some point, we might just move to AWS [for monitoring]; it's been going in cycles for us. We try the AWS tools and realize it's got some limitations, and we go back to Kibana."
- "Amazon's dashboarding is a lot better now than it was so, at some point, we'll switch to purely AWS in the observability area; we're getting pretty close in some areas. Right now we're pumping data out of their observability [tool], CloudWatch, into Elastic, particularly web logs. But, at some point, I would imagine we'll stop using Elastic for that."
- "New Relic has the benefit that they have the client side of observability, not just the server side—that's their key [competitive] twist. They started on the client side and worked back to the server. Whether that's valuable to you or not is a complicated discussion."
- "Splunk is also obviously a competitor."
- "AWS closes the gap all the time because they don't just look at [a problem]; they ask [users] what features they want and, over time, they converge. It's very hard for a smaller vendor [like Elastic] to keep up because there's this curve where AWS is moving closer and closer to [competing] features and sometimes they go past you. And that's where Elastic is in trouble."

> **Amazon's dashboarding is a lot better now than it was so, at some point, we'll switch to purely AWS in the observability area; we're getting pretty close in some areas.**
>
> *Solution architect for a national TV broadcaster in Asia Pacific*

- "If Amazon goes past Elastic in features, which they might in the ML space particularly—it's incredibly hard to compete with Google and Amazon in that space. If you want ML features, which you would in security, for sure, and you probably would in observability, and you definitely do in search, then, at some point, even if you've got solution architects who aren't super advanced, then Elastic [is facing severe headwinds]. It's a shame, because I think Elastic is a very well-run company and I like the people a lot."
- "Elastic is a genuinely good vendor and great to work with. But because observability and search are so core, Amazon and Google can't not do something about it. Solutions that are decoupled from those [cloud] infrastructures are never going to work as well as ones that are deeply built into the infrastructure. The weakness that Elastic is always going to have is that you have to set up all these bridges to get the stuff into Elastic from AWS or Google."

2) Oscar Narvaez, tools and analytic monitoring leader for Entel, a South American telecommunications firm

One of Elastic's key advantages is that is open source, honed by its developer community into a superior solution to competitors. Entel moved to Elastic from Splunk as part of its shift to the cloud because Splunk's licensing model was going to be too costly based on projected data consumption. Entel chose Elastic's paid version to get its machine learning component at a time when the company was moving to a more analytical monitoring model.

Deploying Elastic

- "I've been working with Elastic since 2018 and I've really had a good time working with them as a services provider, as a platform, and as a technology."

- "Currently we have a platinum license. We are growing in capacity for observability and machine learning and expecting to use [Elastic] security for more extended use cases."
- "One of the key advantages is that Elastic is open source and the Elastic community makes it that a lot of people are contributing to it. The Elastic team has done a great job developing the platform and they are continually releasing new features and new versions of the platform and all the tools around the Elastic suite. They help people and companies develop use cases."
- "The open-source aspect enables a huge community to continue developing the product. There is always feedback because so many people are using the product. This is one of the most important aspects that will help their technology continue to grow and make many people adopt the technology for many use cases."
- "It is not just that Elastic is open source but it works really well to ingest and process data and to perform search. It is very high performance. I've seen other tools and they are not based on open source. They just don't have the same high level of performance as Elastic."
- "My decision to use the paid version was based on our plans for the future because we were moving to the cloud. After reflection, we decided to spend less time installing, deploying, managing, and maintaining the tools and we moved to the cloud. We were able to stop spending time on product configuration and maintenance to instead having the cloud service. We invested in spending our time on development inside the platform, for our own use cases—for analytical monitoring and for security."
- "We started using Elastic as a [free] open-source solution. Our main use case was for observability—transactional monitoring. We used Splunk before as our main solution for monitoring. However, their licensing model was based on the amount of traffic that we consumed. We were transforming and growing and we expected to increase our transaction traffic at least five-fold in terms of the amount of data that we would be capturing. This is why we decided to try another technology, Elastic, and, after an initial assessment, we moved completely to Elastic."
- "Elastic does most things very well. One suggestion might be that they could do cloud hosting on a less costly cloud than Google or AWS. Those are the biggest cloud providers. I wish they would extend hosting to other cloud providers to open the accessibility to people who might find Google and AWS too costly."
- "We currently have AWS hosting our cloud services."
- "The key reason we decided to move to the paid version was the machine learning module. It was critical for us because we decided to move to a more analytical monitoring model. This was along with our strategy to move to the cloud."

> **The open-source aspect enables a huge community to continue developing the product. There is always feedback because so many people are using the product. This is one of the most important aspects that will help their technology continue to grow and make many people adopt the technology for many use cases.**
>
> *Oscar Narvaez, tools and analytic monitoring leader for Entel, a South American telecommunications firm*

Enterprise Search

- Did not discuss.

Security

- "I haven't assessed Elastic's security tools as much. We also work with Splunk. Here, too, Elastic's open-source technology is a key advantage while, on the other side, Splunk's licensing model is a disadvantage."

Observability

- "We consider [Elastic] a key provider for observability technology. We use almost all the features they have in observability—observability APM, log, metrics. We also reviewed security but it wasn't as critical for us in our team's IT operations."
- "Splunk is one of the main competitors. It has a similar product in observability and security. I also researched other tools even if they don't work exactly in the same way as Elastic and Splunk but they are good products that can solve some of the use cases. For example, New Relic is a good APM platform. Zabbix is also a good platform for monitoring and observability. Datadog is another good tool for observability."
- "The issue with Splunk is their business model, where the license model was based on our amount of traffic."
- "Elastic's differentiation over these [competitors] is their open-source community. Before we moved to the paid version where we have support from Elastic, we were still able to solve a lot of issues by interacting with the Elastic open-source community."

3) IT executive with a healthcare company

Elastic's platform is fast and can handle large amounts of different data types but it requires a lot of computing resources and takes expertise to manage once deployed. This source's company is using the free version of Elastic but, following Elastic's recent licensing model change, the company is considering switching to the paid version to have access to the distribution rights. An alternative under consideration is to switch to Amazon's Open Distro but the lack of support is a concern. Elastic's single-stack architecture makes the platform simpler to manage but is not a major advantage.

Deploying Elastic

- "We've been considering [paying for] Elastic for more than three years. Because we're in healthcare, the IT development aspect is lengthy because of regulatory approval. We have been actively developing on the Elastic platform for about one-and-a-half years."
- "We are using it purely self-managed."
- "For my personal use at home, I use the Elastic Cloud. I only pay $20 a month for their most basic system. With this, I get additional features that are in the platinum license and that is a lot of value. There would be no way for me to get that [value] if I were to deploy it in my home setup unless I would rebuild my database every 30 days, and that would be a headache."
- "We would like to go to the paid version because of the distribution rights. That is because, as a vendor, we are not allowed to sell the product as a service because of Elastic's new licensing model. We would get the paid version to get the license to sell the product as a service."
- "The decision will be based on cost and whether we can offset the cost with the business value from reselling it."
- "Elastic's platform is fast and it can ingest and process tons of different types of data—log data, observability data, and metrics. Those are the most important aspects for us."
- "I find it to be [computing] resource intensive, especially if you need to scale it up. That could be due to the nature of our design and implementation. But also, personally, I find that if you don't give it the right amount of resources, it can suffer."
- "Elastic also requires human resources. The learning curve is steep. It is very quick to set up and use but, in order to tweak it and get it running well, there is a lot to do and learn as well."
- "Before the change in Elastic's licensing model, it would have been OK for us to distribute products created with their services. AWS' own version of Elasticsearch, Open Distro, is essentially close to the same thing, but it is under a license that is freely distributable and installable. We are, therefore, also looking at Open Distro."
- "It comes down to a feature set and the supportability. Because Open Distro is a community effort, there is no real support available for it. If there are bugs, there is no way to know when or if it will get fixed or if we can do the work ourselves, which would be another huge initiative to look into."
- "The advantages of Open Distro are that we can contribute to the project but it is not a support model that too many enterprises are willing to adopt, especially in healthcare."

> **Elastic's platform is fast and it can ingest and process tons of different types of data—log data, observability data, and metrics. Those are the most important aspects for us.**
>
> *IT executive with a healthcare company*

Enterprise Search

- Did not discuss.

Security

- Did not discuss.

Observability

- "The biggest competitor to Elastic in observability is, in my opinion, InfluxDB. It is an open-source project but offers commercial options as well. They do similar things to Elastic. We did consider them but, when we first started creating this project, they did not have all the features that Elastic had. Elastic stood out because it could look at metrics data and also log and text data."
- "Elastic's strength in observability is that it can integrate into a lot of different components throughout an enterprise, like with the Beats applications—Filebeats, Metricbeats, Heartbeats; they all work well with different components. There's practically nothing we can't plug it into."

- "The downside is managing a lot of that data and making sure that you get data critically at a large scale. It is very easy to set up and run with but we have been having scaling issues. It needs a large amount of hardware."
- "We do use InfluxDB for some other things and sometimes it's a little faster. I would say they are next in line after Elastic."
- "I like it that everything [in Elastic] works together really well but [the unified back end] is not the biggest selling point for me. We can use different components and cut them up and use them in different places, as well, but the unified back end makes it a little simpler to manage."

4) Ivan Ninichuck, freelance security consultant

Elastic's acquisition of Endgame is proving valuable, especially for its addition of event query language, a game-changing advance in the ability to correlate security events. Elastic's security suite is still in development but eventually should prove to be better than competitors like Azure Sentinel, IBM, and Splunk. Elastic's new licensing model will not affect customers who pay for Elastic, since they recognize the value. But users who choose Amazon's free version because it is now the only completely open-source product will be hurt because Amazon's offering is severely lacking. Elastic customers tend to increase their spending with Elastic because of the company's free trials of paid features, which convince users to eventually pay for them. New customers especially value Elastic's machine learning capabilities.

Deploying Elastic

- "Most of the deployments [of Elastic] are in the cloud, probably at least 70%."
- "Elastic Cloud provides a very high utility value because you don't have to manage the stack yourself. For example, if you're a security service provider, you don't want to spend time maintaining the stack because your main focus should be security. An Elastic stack is not easy to tame on premise."
- "During my time as a freelancer, I always recommended Elastic Cloud, and use it for my own work. I have seen others self-manage a stack in a general cloud setting as well. The benefits for security projects of using a managed service like Elastic Cloud are immense. I think most security products are heading towards SaaS offerings over on-prem in the future."
- "Elastic brings in a large variety of data and makes it actionable. There are areas like easy multi-tenancy and more out-of-the-box features that I would like to see them go further with. By multi-tenancy, I mean they should be able to have multiple customers' data sets going to Elastic and being able to keep them segregated easily. Originally, they didn't have built-in multi-tenancy, but now they have Kibana Spaces and we [in the user community] are pushing for more features with the Elastic Agent. They have made some strides."
- "The ease or difficulty of the initial deployment has changed in 2021 compared to 2019. There's a huge difference."
- "In 2019, it was highly difficult. You still mainly had to use Logstash as the ingest pipeline. Everything had to be configured on the servers. Even though there was central management, it wasn't widely used and it wasn't that easy to use. We didn't have the out-of-the-box features that we are now starting to take for granted."
- "Now, in 2021, it is easy. The Elastic Agent replaces all the Beats and you can manage it centrally from Kibana using the Elastic Agent. It's a huge game changer. In 2021, it also includes the new Elastic Endpoint Security. It's like using a fast food menu."
- "Operating and maintaining the entire stack on premise has a medium to high difficulty level. It involves a lot of server management and managing memory resources. To have it on premise, you need somebody who's been trained. On cloud, you don't have to worry about it because it's managed for you. I use cloud."
- "Most clients I've spoken to have been happy with the costs. If you compare Elastic to other products, it would cost much more to get the same amount of visibility and insight. It's a win."
- "[Elastic's] machine learning feature, which is paid, is definitely worthwhile. For security, it's easier to create baselines when you have anomaly detection. It is going to pay off in the end."

> **Operating and maintaining the entire stack on premise has a medium to high difficulty level. It involves a lot of server management and managing memory resources. To have it on premise, you need somebody who's been trained. On cloud, you don't have to worry about it because it's managed for you.**
>
> *Ivan Ninichuck, freelance security consultant*

- "Some of the features that used to be paid before are in the free tier now. For example, Watcher, the old alerting platform, used to be a paid feature. Now, the Elastic detection engine is on the free tier."
- "Clients generally increase their spending on Elastic. When a client sets up a cloud account, they get to try out some features even if they're not on a high support tier. That encourages clients to increase their spending for some of the things they tried. As an example, you get a small machine learning node when you sign up for a trial on the cloud. That way you can see what they do and how much value they add. Clients tend to end up saying they like it and they want to go to the next tier."
- "I think the impact [of Elastic's licensing model change] is going to be negative for users who allow themselves to be misled by Amazon. I'm on the side of Elastic on this one. Although the license they changed it to is not technically recognized as open source anymore, it is still open code. You still have a tier of license where you can use the code, just like you could before. You just can't offer it anymore as a service and pretend it's your own product. Unfortunately, Amazon has used this to create a mess and now they have the only true open-source version of Elastic."
- "I've used the [Amazon] Open Distro and I've serviced customers that use it. It's like buying a Ferrari and having the engine torn out. That's what it felt like when I was using it. All the best features that Elastic has been adding are not there, things like the detection engine and EQL. A lot of users are going to get duped into thinking that they need to use the Amazon version for certain projects and they're going to be missing out."
- "I don't think it will hurt Elastic in the long run but I think it will hurt the community. The corporate customers that are using Elastic Cloud or the ones paying the licenses for using it on premise are going to keep paying because they can see the product is good. The smaller users who choose Open Distro vs. the Elastic version are going to get hurt and their security is not going to be as good. I think this will mean more ransomware attacks succeeding because Elastic Security was not there to stop them."

Enterprise Search

- Did not discuss.

Security

- "The major strength of Elastic's security solution is its ability to correlate multiple events over time. They just introduced EQL, which was developed by Endgame before [Elastic] acquired it. It is mind blowing. It's in the stack now. The user community has been going crazy over it. It's the most exciting thing that's happened for years in Elastic security. It enhances the game when dealing with alerts and investigations. It's their biggest strength easily. It's very exciting."
- "EQL has revolutionized the ability to correlate security events. It's made up for the gap with sequel-based databases. The sequeling and no-sequel people used to like to tease each other. The biggest criticism of Elastic was that their query languages were not very good at correlating events. With Endgame and EQL, and the Endgame engineers now becoming Elastic engineers—who are very active in the community channel—it has changed it completely."
- "The free tier Elastic Endpoint Security can now isolate a host. This used to be a paid Endgame feature only."
- "In terms of challenges, because everything is so recent, there still needs to be more testing to see where the blind spots are. It's a process over time. The Elastic SIEM really only took off last year. Elastic Agent is still in beta testing. Hopefully, it will move into general availability later this year. Time is the only weakness until everything gets looped together."
- "The industry also needs to get stronger here. If one product has these blind spots, it's going to be in other products as well. For instance, I noticed there are major blind spots in detection rules since the SolarWinds [Corp./SWI] and supply chain attacks. We need to find these blind spots and fix them."
- "I do view Elastic's security suite as a differentiated offering. It has a wider visibility than other offerings. It's easier to ingest multiple data sources and it is easier to work with the data. For example, when you are developing detection rules, it feels more interactive for your needs. There's more customizability. It doesn't feel like it was created artificially by a product team. You can customize it more and you can play with it a lot more."
- "Elastic's key competitors are Azure Sentinel, IBM—which has a leading SIEM offering—and Splunk. Splunk is losing but there are still some big Splunk users out there."

> **The major strength of Elastic's security solution is its ability to correlate multiple events over time. They just introduced EQL, which was developed by Endgame before [Elastic] acquired it. It is mind blowing. … The user community has been going crazy over it.**
>
> *Ivan Ninichuck, freelance security consultant*

- "Elastic has advantages over these others. Gartner had Elastic low in their quadrant but that's because so many of the parts that have made [Elastic's] security solution come together have only been introduced in the last year or so. They're on the crest of the wave and not yet matured. Elastic is in an interesting position."

Observability

- Did not discuss.

5) Software developer using Elasticsearch at a major retailer; repeat source

There are no competitors that can replicate the functionality and scale that Elastic provides. This source's company is using the free version of Elastic and self-managing it. The company might consider the paid version if the team wants to use some features like machine learning. Solr and InfluxDB are comparable to Elastic in enterprise search but Elastic's integration of Kibana provides valuable additional capabilities.

Deploying Elastic

- "I have been working with Elastic since 2015 [at a former company]. It replaced Splunk."
- "I started with basic Elasticsearch and then moved on to use Kibana heavily. I also used Timelion quite a lot."
- "We are using the free version in my team and it is self-managed."
- "So far, just for my team, the free version is sufficient; it has been incredibly helpful. If, in the future, we want to use some of the paid features like ML, I might push my manager to see if we can get the paid version as well."
- "[Elastic] has been evolving and making things faster. With the newer Kibana instances, we can stop heavy running queries, which can bring down clusters. Functions like this are quite helpful on top of all the marvelous options they offer."
- "However, for metrics—time-based logs of statuses or system logs—InfluxDB with Grafana beats Elasticsearch and Kibana with performance. That is something Elastic can look into to see if they can make it more efficient."

> **Just for my team, the free version is sufficient; it has been incredibly helpful. If, in the future, we want to use some of the paid features like ML, I might push my manager to see if we can get the paid version as well.**
>
> *Software developer using Elasticsearch at a major retailer*

Enterprise Search

- "Not that I am aware at this point [can anyone else replicate Elastic's enterprise search at the same scale and functionality]."
- "I have not evaluated Amazon's [Elasticsearch] service. However, last time I checked, the kind of computation it offers, our team might need bigger storage, which can increase cost compared to hosting it on prem."
- "While Elastic provides search comparable to Solr or InfluxDB, its integration of Kibana providing the capabilities to efficiently add filters over a dashboard really helps in triaging issues and for monitoring purposes."
- "Solr or InfluxDB providing better visualizations over their backend data could be something which can compete with Elastic."
- "One thing that takes us quite some resources [with Elastic] is aggregation—especially transactions per second, where it becomes extremely slow and fails at times over longer durations."

Security

- Did not discuss.

Observability

- Did not discuss.

Feb. 6, 2020, summary: Elasticsearch is a powerful search engine that has been improving with each version. Its ability to scale horizontally and the platform's Kibana visualization tool add to its value. Other tools, however, can be a better fit, depending on a company's needs. The support Elastic offers with the paid version of its software is terrific but, for some users, the free version is fine. Elastic's documentation and its active user community make it easy to switch from another platform.

2) Industry Specialists

The four sources in this silo were generally negative about the value of Elastic's paid features and its ability to stand out from competitors. Elastic's underlying platform is easy to get up and running, two sources said, by making it relatively simply to configure search clusters, create API keys, and begin pushing data. But its paid version is not very compelling, one source said, and Elastic is having a hard time differentiating itself from Amazon and others. One source, an enterprise search consultant who was enthusiastic about Elastic's platform 18 months ago, said all of his clients are now using the Amazon version of Elasticsearch in AWS. Amazon's product has made significant strides with features that Elastic charges for, such as security and user authentication, he said. Elastic's new licensing model will not alter the competitive dynamics, two sources said, as those using the AWS version will continue to do so and those wishing to distribute versions of Elasticsearch will use Amazon's forked product. The license change has sparked some distrust of Elastic among developers devoted to the open-source model and some of those people may shift toward working on new features for Amazon as a result, according to one source. Three sources said they are seeing vendors move toward a combined solution for observability but two said Elastic is not among the leaders in this segment. One source said Elastic lags others in application performance monitoring, in particular, and requires significant staffing resources to manage. Elastic's single-stack technology is not a differentiator, according to two sources. Big companies use anywhere from two to six different vendors for various observability functions, one source said.

Key Silo Findings

Deploying Elastic

- 1 of 4 said most of his clients use the AWS version of Elasticsearch.
  - He does not have any clients currently using Elastic Cloud.
  - Clients are choosing the AWS version largely because it is easier to deploy Amazon services once in the AWS ecosystem.
  - Amazon's version has improved significantly in areas that Elastic charges for, like security and user authentication.
- 1 said Elastic's platform makes it easy for developers to configure search clusters, create programmatic API keys, and start pushing data.
- 1, representing a competitor, said there is no area where Elastic truly excels beyond being easy to get started with.
  - Elastic's service on top of the cloud is more costly and less flexible.
- 1 said Elastic's paid version offers nothing with significant appeal.
  - Its hot and warm architectures are available from Amazon's version.
- 1 said he sees no evidence Elastic can differentiate itself from Amazon.
- 2 said Elastic's new licensing model is unlikely to help the company in its fight with Amazon.
  - Companies using the AWS version will likely stick with it.
  - Customers who want to resell Elasticsearch will use Amazon's forked version.
- 1 said the licensing change is causing some trust issues with developers, who may choose to contribute to Amazon's version instead, since it is fully open source.

Enterprise Search

- 2 said Amazon's version is pretty comparable to Elastic's in core search functions.
  - 1 said Amazon has an advantage because of the easy integration with other services within AWS.
  - 1 said Elastic cannot compete with Amazon on cost because it does not manage its own data centers.
- 1 said Elastic's search offering is no longer differentiated from competitors.
- 1 said that, while it is possible to run Elastic's version in the AWS cloud, it takes a lot of effort that few would bother pursuing.
- 1 listed ChaosSearch as a competitor for applications that are not latency sensitive and InfluxDB and Timescale as competitors for time-series data.
- 1 said his company is a Microsoft shop and, thus, uses an Azure product for enterprise search.
  - The company is satisfied with the solution.

Security

- 1 said his company switched from Splunk to Dynatrace for security.

Observability

- 3 said many vendors are pushing toward an all-in-one solution for APM, monitoring, logging, and security.

- 2 said Elastic is not a leading vendor for observability.
  - 1 said they are far behind modern APM solutions and, because their offering is not fully managed, it requires teams of people to run the infrastructure.
    - Companies with talent savvy enough to do so can just as easily run Amazon's free version of Elasticsearch and build their own additional pieces.
- 2 said Elastic's unified backend architecture is not a differentiator.
  - 1 said that, in practice, companies will run multiple clusters for things like logs, search, and APM, so there is no advantage to Elastic's single-stack structure.
- 1 said companies are most often using at least two vendors for various observability tasks, rather than consolidating on one. Some are using as many as six.

1) Developer for an enterprise search consulting firm; repeat source

Amazon has emerged as a real roadblock for Elastic's paid subscriber growth. This source's entire client base is now using Elasticsearch in AWS and none are paying for licenses from Elastic. The source was much more bullish on Elastic 18 month ago, when he said most clients had an Elastic license, rather than relying on the free Amazon version, in order to get faster updates, key features, and better support.

Deploying Elastic

- "I have clients like [one the of the world's biggest auto manufacturers]. I also work for the government of Canada. They were already using AWS Elasticsearch and so asking them if they wanted to use Elastic Cloud [didn't make sense]. They were already on AWS everything."
- "Most clients I have are already on AWS. Yes, I see this impacting Elastic's growth. Since [18 months ago], I don't actually have any clients that use Elastic Cloud."
- "It's just the [Amazon] ecosystem. It's like you purchase an Apple [Inc./AAPL] product—you're in the ecosystem and it's easier for you to deploy other services within AWS, including access control and the policy system. If you don't, then you're stuck with, 'Here's the user name, here's the token, and here's the password—that's the Elastic stack cloud there.' That URL is open to the public, as well, and sometimes clients don't want that to be an internet-facing service, even if you have authentication."
- "I think the new [Elastic] licensing model will have no [immediate] impact. Cloud users will likely continue to use Elasticsearch within their cloud ecosystem for more secure firewalls. Most clients use AWS and, thus, will stick with AWS Elasticsearch—Open Distro."
- "No, not at all [will the new licensing model steer users from Amazon's version to Elastic's]. The AWS services integration will keep users there and they will not likely move to use Elastic that is outside of the firewall perimeters."

> **The new [Elastic] licensing model will have no [immediate] impact. Cloud users will likely continue to use Elasticsearch within their cloud ecosystem for more secure firewalls. Most clients use AWS and, thus, will stick with AWS Elasticsearch.**
>
> *Developer for an enterprise search consulting firm*

- "What I would be afraid of as a user [as a result of Elastic's new licensing model] is what else is [Elastic] going to change that's going to lock me out down the road? Now I have to pay more [for services that were once free]. AWS Elasticsearch is managed, so clients don't have to worry about whether they will have features missing [down the road]."
- "The open-source attributes [of Elastic] were blurred in the past and with the new so-called Elastic license, as opposed to the Apache 2.0 license, it can be confusing. Understanding that Elastic as a company has to make money, this [licensing change] is causing trust issues with open-source developers and contributors. They may contribute to [Amazon's] Open Distro instead and make new features there."
- "There's definitely some conflict between AWS and Elastic. Most clients that use AWS cloud, for them to use Elastic as a source for Elasticsearch, I'd say it's more rare. It's not the preferred method because it's like a two-vendor account, billing wise; the client would have to pay two different [companies] to establish everything."
- "For me, most of my [client] setups have been using AWS Elasticsearch, just because it's there and ready to use. To use Elastic Cloud, it's becoming less common for me."

- "I think it's also because [AWS'] Open Distro for Elasticsearch is so much more advanced now that you would question whether clients really need to use Elastic Cloud. If you use Elastic Cloud, you're looking for something that's the latest and greatest, [something] that's not out yet. Then, yes, you might want to use [Elastic Cloud]."
- "But for most things that clients would use [Elastic Cloud] for, it's there [in AWS]. And I think AWS Elasticsearch now is not from Elastic; it's the Open Distro version."
- "Open Distro is also an open source that is supported by Amazon and it's fully open source. It has a lot of features like security, user authentication, and a bunch of stuff that Elastic used to charge for. And when you're using AWS Elasticsearch, it uses that in the back end."
- "That's why Elastic is not really going to make any money off those users who [choose] AWS Elasticsearch."

Enterprise Search

- "The most common uses are for the search engine from Elasticsearch stack only and AWS Elasticsearch does a pretty good job. Upgrading [within AWS] is easy and has tight integration within the same cloud ecosystem with commonly used features."
- "Elastic does have the marketplace that you can run Elasticsearch within the AWS but it takes a lot of effort to get that running. And that level of effort is usually not something anyone would pursue, unless they really love Elastic."

Security

- "There was one project I worked on [with a security component] but we used our in-house [security tools] and not Elastic's. That was sent to Elasticsearch stack and with that I had to implement some extra things to allow [that integration]."
- "That was implemented using the Elastic Cloud but it was [more than 18 months ago]. Since then, all my clients have been AWS. It was just easier to go with AWS rather than set up something [with Elastic Cloud]."

Observability

- Did not discuss.

Feb. 6, 2020, summary: Use of Elasticsearch and other enterprise search engines is growing, especially as a replacement for SQL database indexing. Running Elasticsearch in the cloud—either with Elastic Cloud or AWS—is a more cost-effective way to deploy it than managing it on premise. Some clients prefer Solr as a search engine, but Elasticsearch is easier to get started with. While some clients run Amazon's Elasticsearch to take advantage of single billing and, possibly, discounts as AWS customers, most have an Elastic license to get faster updates and features like Snapshot and Restore. Elastic also offers much better support than Amazon.

2) Senior software engineer for a competing observability platform

Elastic's cloud service is costly and not easily configurable. There are no real advantages to the paid version over the free. Elastic's recent licensing model change is not likely to have any impact. Elastic does not have much differentiation in enterprise search and many organizations use the open-source version for it. Elastic would need to have a fully managed product that is price friendly in order to be competitive in observability, where its single-stack architecture is not a useful advantage.

Deploying Elastic

- "Elastic's platform is, by far, one of the most approachable. For a developer to configure a search cluster, create a programmatic API key, and begin pushing data, it's very simple."
- "Unfortunately, beyond that, it's hard to imagine an area where Elastic truly excels. Their service on top of the cloud is more costly and less configurable, and their sales process pushes you towards a costlier enterprise installation."
- "[Elastic's paid version has no key advantages] that I've found. I don't care for multi-cloud support and the hot and warm [storage] architectures are well supported by Amazon Elasticsearch service."
- "[The impact of Elastic's licensing model change will be] probably nothing. For people looking to run Elasticsearch themselves, the SSPL [Server Side Public License] doesn't change for them because those users are not offering Elasticsearch as a product. For companies that do resell Elasticsearch, like ChaosSearch, they'll just use the Amazon fork of Elasticsearch."
- "Elastic will have to prove it can add value in a way that Amazon can't and, so far, I've seen no evidence demonstrating they can deliver on that."

Enterprise Search

- "I've built SaaS products that use Elasticsearch [but] I don't have a ton of experience using the pure enterprise search features."
- "Yes, [competitors can replicate Elasticsearch's capabilities and scale], since their predominant offering is search, which isn't something they seem to differentiate on anymore, as other services can use the open-source fork."
- "Yes, Amazon's offering is competitive in my experience. Both Elastic and Amazon don't offer a fully managed Elasticsearch product and AWS is able to compete on cost in ways Elastic can't because Elastic does not manage their own data centers—they rely on AWS, GCP [Google Cloud Platform], and Azure."
- "ChaosSearch for applications which aren't latency sensitive [is a competitor]. InfluxDB and Timescale seem to be making inroads in time-series data, which is a niche Elastic has supported for a long time."

Security

- Did not discuss.

Observability

- "All major vendors are striving to be a one-stop solution for APM, monitoring, logging, etc. I think Elastic could make a play to be the underlying support infrastructure but, so far, I don't see a major play for them in the [observability] space. They're just too far behind modern APM solutions and their offering isn't managed. Companies have to have entire teams of people dedicated to running the infrastructure and they don't want to do that."
- "Teams technically savvy enough to implement and run an ELK stack for APM, monitoring, logging, etc., are technically savvy enough to cut costs by using the open-source version of Elasticsearch and running it themselves. That continues to be the biggest challenge to Elastic. They need a price-friendly, fully managed product in order to remain competitive."
- "[Key competitors in observability include] Honeycomb, Datadog, New Relic, Dynatrace, Splunk."
- "[Elastic's backend architecture] is not really unified. That seems to be mostly marketing speak, in my opinion."
- "Their pitch is that you can use one deployment [and] turn on enterprise search, security, and observability with one click. And it's true that you can do that. But nobody would do that in production."
- "Elasticsearch clusters aren't semi trucks or container ships. They're more like F1 cars. They require a team of experts tuning them just right to be at their maximum performance. You can't just throw a logs index next to your enterprise search index in the same cluster."
- "First, they'd be competing for resources, leading to contention and performance degradation. Secondly, the search and index patterns are way different. Enterprise search is more read-heavy, so you'd want very fast storage and search nodes."
- "Logs and APM data is time series—it's indexed very quickly and often you care about looking at logs in the last 30 minutes very quickly. The volume is huge and if there's a delay—due to contention—you might never catch up with your application."
- "You also can't afford to keep everything in NVMe SSD drives, so you'd want a hot-warm-cold architecture here, which isn't suitable for enterprise search. Since you're going to run multiple clusters for logs, search, and APM, you might as well consider different vendors. And then, who cares about the unified backend?"

3) IT executive formerly with an education company; repeat source

This source's former company uses Microsoft's Cortex for enterprise search and Dynatrace for security and observability. As a Microsoft shop, the company prefers Azure-native products. Additionally, it gets an education discount from Microsoft that would make it difficult for other platforms to be competitive. Dynatrace has become a one-stop shop for security and observability, providing the "Cadillac of products" in those segments.

Deploying Elastic

- Did not discuss.

Enterprise Search

- "We use an Azure-native product, Project Cortex, [for enterprise search]. It uses AI. We did models to categorize and section data. Now, for example, if I want to do a global enterprise search for a word in every document and video and audio file that's stored in the organization, this tool lets me do that."
- "We are very satisfied with it. We started with the pilot in 2019 when it was still in development and then became a paying customer."

- "I found Cortex intelligent because it is able to maintain my databases without needing too much interaction. When you set up Cortex and build your models, it continually scans the data. When we were developing it, it was a little convoluted for the models but they created good wizards and now it's easy for the average administrator to set up."
- "We didn't look at anything else because, for us, it was the only thing in the market. We are a Microsoft shop and tend to use Microsoft in everything. I like to stay within the ecosystem. This was also a good setup for us because of the education price breaks from Microsoft. Unless there is a very large price gap, we don't look elsewhere."
- "I'm aware of Amazon's free Elasticsearch product but I haven't used it. We don't use AWS."
- "Whenever Amazon enters a market, there's always a pricing war. I'm guessing that Elastic will hold their superiority. They should play that up and justify their prices."

> **We use an Azure-native product, Project Cortex, [for enterprise search]. … We are a Microsoft shop and tend to use Microsoft in everything. I like to stay within the ecosystem.**
>
> *IT executive formerly with an education company*

Security

- "I switched to Dynatrace's new security module [from Splunk]. It does an amazing job scanning the code before it goes into production. Before, we didn't have a way to become aware of these types of vulnerabilities until I ran a penetration test and a report, which I only did twice a year. Now we get continual scans of our code and the tool sends alerts whenever it finds something that needs to be corrected. The code we ship out to production is clean and vulnerability free that way."
- "We didn't look at competitors. We were a Dynatrace shop and my main driver was to not have multiple tools. When I have a tool, I want to maximize it to get as much out of it as possible if it does it as well as the competition. For security, I had no alternative. The only one I was aware of was Snyk and their product is so phenomenal that it's what Dynatrace uses on their backend. However, I couldn't afford to deal with Snyk directly because of their sky-high minimums. With Dynatrace, I have the Cadillac of products."
- "At the moment, we're not big on endpoint protection. We are using Microsoft Intune, their mobile device management. We also often use it for desktops, as well. We don't do endpoint protection from the customer perspective, only internally. Intune is perfectly satisfactory for that."

Observability

- "I do see a convergence [between tools like APM, infrastructure monitoring, logging, and SIEM]. Dynatrace is already close to being a single stop for all of that. They just added their automation module which brings DevOps automation within their realm as well. If, for example, you use [Atlassian Corp. PLC's/TEAM] Jira for ticketing, that makes a DevOps loop to totally automate releases."
- "We use Dynatrace for observability. Previously, we used New Relic. We used Splunk for just the logs."
- "Dynatrace stands out as better than New Relic by far."
- "A unified back end is important for any product regardless, though I haven't looked at Elastic. Being cloud native would be a great additional marketing tactic for Elastic. It's something I look for rather than choosing a product that was converted from onsite to cloud."

Oct. 30, 2020, Splunk report summary: This long-time Splunk customer will be leaving the platform at the end of the year. Dynatrace's log mining capabilities have improved and are up to par with Splunk, so it makes sense to consolidate operations into one product. It is too late for Splunk to become a big player in the observability market, as established companies like Datadog have focused on that segment. Splunk should have remained focused on log monitoring instead of diluting its platform by delving into observability. The capabilities of the native tools that Azure and other cloud providers sell are not up to par with third- party tools like Splunk. Finding trained workers is not an issue with tools like Splunk or Dynatrace because they are more easily accessible than older tools, like New Relic, that required a lot of human resources. Splunk is reasonably priced for what it provides.

4) Executive with Sematext, a competing observability software vendor

Elastic is far from being a leader in the extremely competitive observability market and its single-stack architecture does not make it stand out from the crowd.

Deploying Elastic

- "My company competes with Elastic and others in the observability space."

Enterprise Search
- Did not discuss.

Security
- Did not discuss.

Observability
- "Yes, [I am seeing a trend toward] multiple solutions in one. [We were] actually the first vendor to offer infrastructure monitoring and log monitoring in 2013 and then infrastructure monitoring and log monitoring plus transaction traces in 2015. A few years later, the industry started calling this 'the three pillars of observability.' This is common now."
- "Elastic is far from being alone or the leader there [in observability], in my opinion. I am not aware of Elastic having anything in their offering that's a differentiator from other similar vendors. Competitors include Datadog, New Relic, Splunk, Sematext, Logz.io, Sumo Logic [Inc./SUMO]."
- "Companies will always have tools of a similar kind, sometimes complementary, sometimes simply overlapping. I saw the same when I was in the enterprise search space 10 to 20 years ago. Having just one solution that does it all is always a goal, but it's also Utopia."
- "In the monitoring and observability space, there was no product that offered multiple types of modern monitoring solutions until 2013. I remember people not getting that idea. Now, things have changed and people do get the value of an observability platform offering different types of monitoring in one. That's why we offer four in Sematext Cloud and will be adding more. People get that now."
- "I haven't seen or heard anything that would make me think [Elastic's unified backend architecture] is anything special. If they use only their own software—just Elasticsearch—to store the various types of data, one may think that that's nice and neat but it's not really optimal because Elasticsearch is not the best choice for storing certain types of data. We've tried it because we thought we could use Elasticsearch for everything but we found much better back end for storing certain types of data."
- "Also, in the end, the end users don't really care what's behind the scenes as long as their experience is good and it doesn't cost them an arm and a leg. And Elasticsearch is expensive to run, often the costliest part of observability infrastructure."
- "Competitive [issues among observability vendors] include price; ease of use, UX [user experience], adoption; ability to go from high level to detail and troubleshoot; a suite of integrations with various data sources; outputs; ability to handle different log formats; and out-of-the-box value."
- "No universal answer [as to whether companies are typically deploying a complete observability solution from a single vendor or multiple best-of-breed pieces]. I often hear at least two [vendors being deployed]. Very common. I wouldn't be surprised if, in larger organizations, I'd find half a dozen if I dug."

> **Elastic is far from being alone or the leader there [in observability], in my opinion. I am not aware of Elastic having anything in their offering that's a differentiator from other similar vendors.**
>
> *Executive with Sematext, a competing observability software vendor*

3) Elastic Partners

Elastic offers a lighter and more agile way to approach logging and security incidents management than other enterprise platforms, according to the one source in this silo. Enterprises value it because it can be deployed in small use cases as well as large ones and is effective in both. Elastic meets expectations for cost savings as long as companies have the human resources talent to customize the platform for their specific use cases. Two main competitors are Splunk and ArcSight but customers using Elastic find it is a differentiated offering and tend to increase spending on Elastic. To grow in the face of pressure from Amazon's competing product, Elastic will have to find ways to keep adding value on top of the open-source product, such as enterprise support features or alliances with other cloud providers. Amazon's free version of Elasticsearch can benefit Elastic by bringing new users to the platform—people who eventually will pay for Elastic's version.

Key Silo Findings

Deploying Elastic
- 1 of 1 said new deployments of Elastic are generally self-managed rather than in the cloud.
- 1 said Elastic's platform is a lighter, cheaper, and easier-to-use tool for SIEM than its competitors.

- 1 said some competitors like ArcSight, Cisco, and Splunk have more features but that does not make them better.
- 1 said Elastic meets customer expectations for cost savings as long as the company has the staffing talent to deploy it and customize it properly.
    - Elastic gets expensive for companies that need to hire consultants to deploy or operate the software.
- 1 said the key advantage of paying for an Elastic subscription is the support, something that is a must-have for most enterprises.
- 1 said clients tend to increase their spending on Elastic over time because they find new uses for it.
- 1 said Elastic will have to continue to add valuable features to the base platform in order to fend off Amazon.
    - Amazon's free version will help familiarize users with Elastic technology, something Elastic can benefit from down the line.

Enterprise Search

- Did not discuss.

Security

- 1 said Elastic's advantage in security is its ability to be deployed in small pieces, making it helpful for both small and large use cases.
- 1 said Splunk is Elastic's key competitor in data logging and ArcSight is the biggest challenge for enterprise security.

Observability

- 1 said various tools like infrastructure and application performance monitoring are converging into single platforms but the trend will neither help nor hurt Elastic, as big companies prefer to buy the different elements separately.

1) Development executive for an Elastic channel partner

Deploying Elastic

- "The new deployments [of Elastic] are mostly self-managed."
- "Using Elastic SIEM is a lighter and more agile way to approach logging and security incidents management. It's an elegant solution. Also, it's open source, so there's a community of users around it. It's a different approach from some of the other heavy enterprise software platforms. It's a better and thinner deployment model. Everything is less, easier to do, cheaper, more elegant, and more minimal deployment rather than a big undertaking."
- "I don't know of anything that Elastic doesn't do well. Some other software packages can do more because they are a bigger all-in-one play. Elastic can't shine your shoes but the problems it does solve it does very well and even better than others."
- "Vendors have different approaches. ArcSight is a big player. Cisco also allows you to do some things. So does Splunk. But, in terms of SIEM, Elastic does it just fine. You don't need more than that. Some of the others have more functions built into them but that doesn't necessarily make them better."
- "Yes, [Elastic meets customer expectations for cost savings], but you need to know how to deploy it because it is highly customizable. You need people who are familiar with it and are comfortable in the medium. Apart from that, it does meet client expectations."
- "However, if you can't find those people and you have to sign Deloitte to do it for you, it's not going to be cheap. In other words, you have to know how to deploy it. You can't just acquire the software. You have to know how to deploy it and make it part of your discipline. If you don't have that already, you have to build that capability or hire someone to do it for you, which then leads to a new question about the cost savings. This is especially so if you're leaving a tool that you've been using for a long time and you had a lot of in-house ability to work with it."

> **The advantage of the paid version [of Elastic] is that it is enterprise supported. Large enterprises can use pure open-source product for some things but it's a tough case to make that you're making sure it's up to snuff on everything.**
>
> *Development executive for an Elastic channel partner*

- "One of the things Elastic does well is that it allows for multiple log-in sources. You can use it from a cloud platform or a data center platform. It's easy and they give you a lot out of the box. A lot of people who use it have the capability [to deploy it properly]. This is really important in cases where there's private health data that's involved or

a municipality or government or financial services or private healthcare. That's very important data and if you don't know how to use your SIEM software, you are vulnerable."

- "The advantage of the paid version [of Elastic] is that it is enterprise supported. Large enterprises can use pure open-source product for some things but it's a tough case to make that you're making sure it's up to snuff on everything. When you buy enterprise-supported software, you can get them to vouch for that and so it's auditable. Big enterprises need it to be enterprise software or they cannot use it otherwise."
- "In general, clients increase their spending on Elastic because they expand their use. They usually start off small. Maybe they have a small use case where they have a new cloud platform and they want to synchronize that with their data center platform. Once they get used to it and they figure out how to use it and they've gone through a patch cycle, they want to start expanding."
- "As an example, with COVID, the government needed outsourcing capabilities for call centers. They would use Elastic to do the logging because it was an easy deployment and they didn't have to buy in big time into a new platform. Once they are using it, they make it permanent and then they have to buy all the licenses so they get further into it."
- "Elastic won't be able to stop Amazon from building their own version of search. Therefore, Elastic needs to make lemonade out of lemons—find the differentiators and amplify them. These could include enterprise support features, multi-cloud features, SIEM enhancement, etc. It could also include an alliance with Google Cloud Platform or something else strategic."
- "They also need to realize that if Amazon is standardizing on it, there's a further play. They can take the momentum of that standardization and bring it back to the place where they can add value. Elastic will have to adapt to that change. They will have to find a way to capitalize on the fact that they are going to get a much bigger user base."
- "The Amazon users that would not have implemented Elastic on its own will be implementing the [Elastic] technology [through Amazon's version]. The people who are consuming Amazon's [version] are going to be consuming this [Elastic] product. New people coming into the workforce working at their $40,000-a-year job are going to be seeing the open-source version of Elastic being used constantly. When they grow up, they are going to see that as a standard. That means that Elastic is creating momentum around its way of thinking by creating additional users, even if those users aren't paying Elastic right now."
- "Those users are now captive in the Elastic way of doing things. Every time Elastic adds value in the market, those users then become [Elastic's] market. This is like when people ripped off Microsoft Word when they were 19. They started paying for it when they were 29. But they kept using Microsoft. Microsoft established incumbency and a user group that understands them."

Enterprise Search

- Did not discuss.

Security

- "The strength of Elastic's security solutions is the fact that it can be deployed in small pieces. That makes it accessible. You can use it in a small use case as well as a large use case and it's fully effective in both."
- "The limits of Elastic's simplicity could be considered a weakness. It's a positive feature but it's also a limit."
- "Splunk is a competitor on the data logging side. ArcSight is the big competitor in terms of enterprise security. They are different. ArcSight has less limits but it does more. Splunk is more widely used than Elastic in the market overall but not in the security market."
- "Elastic's security suite is a differentiated offering. This is the feedback from customers who've put a lot of thought into it."

Observability

- "We do see that [convergence of tools] pitched a lot but the effect on Elastic is neutral. This is because there are people who want to use the Elastic approach along with other tools. That's because, in large enterprises, once you choose a tool, you have to make a big commitment. It's not easy to go to a new tool, so enterprises like to break it up a little bit. They like to buy the elements themselves and, that way, they are not as bound to a single tool. They like Elastic because it breaks the hegemony of the big enterprise tools."

4) Competitor Partners

Splunk has more appeal than Elastic in enterprises for which time, security, and out-of-the-box features are the main concern, rather than upfront cost, according to the one source in this silo. Elastic is better suited to companies with access to affordable resources and employee talent, usually outside the United States, because of the customization it requires.

Security tools are not converging with APM, infrastructure monitoring, and logging. Security teams are usually separate from standard IT functions in an organization and use their own tools. It would limit a vendor to build an all-in-one offering and reduce a client's flexibility to decide which parts it wants to add.

Key Silo Findings

Deploying Elastic

- 1 said choosing Elastic only makes sense where inexpensive human resources are available, which tends to be outside the United States.
  - Because of COVID-19, however, companies are becoming more accustomed to deploying new platforms without in-person implementation, which could remove some of the barriers to choosing Elastic.
- 1 said there is a lot of competition in Elastic's key segments.

Enterprise Search

- Did not discuss.

Security

- Did not discuss.

Observability

- 1 said Splunk is more of an enterprise-level tool than Elastic.
  - Splunk will get companies where they want to go faster but at a higher upfront cost, whereas Elastic may be cheaper at the outset but requires a lot of talent to customize.
  - Splunk has more security features desired by big companies, such as role-based access control.
- 1 said Splunk is the right choice when the key criteria are time, security, and features, rather than cost.
- 1 said numerous tools are converging in observability suites but not security, as those teams are generally a separate part of IT organizations with their own budgets and priorities.
- 1 said Elastic's unified architecture is not a differentiator.

1) Professional services consultant for a Splunk partner; repeat source

Deploying Elastic

- "I believe using the Elastic platform makes more sense where inexpensive resources and talent are available but that's not something that can really be found in the U.S. I think that has been a barrier for Elastic. Implementing Elastic onsite in the U.S. would be too expensive. The costs would greatly surpass Splunk's licensing cost."
- "It could also be that we are at an inflection point because, with COVID, customers are becoming more accustomed to in-person implementation not being key to a project. That opens up the path for offshore implementation. I'm speculating but Elastic in this way could take on some projects that would normally be delivered onsite only."
- "Of course, more projects are also moving to the cloud and there's less on-premise implementation. Barriers are changing and when we are past COVID, it may be that no one will return to the office and there will be less need for high-touch consulting."
- "There is a lot of competition in this space. As an example, Splunk's ex-CTO is starting a new cybersecurity company."

Enterprise Search

- Did not discuss.

Security

- Did not discuss.

Observability

- "Although Splunk is in the same market as Elastic, they are really in different spaces. Splunk is more enterprise. It will get you where you need to go faster but at a higher upfront cost. Elastic can do the same but it will require more [human] resources to do it."
- "Also, Splunk has more security features that are important to large companies that are looking to tie certain features in to their existing infrastructure, like RBAC [role-based access control], which controls authentication and privileges that determine who can look at the data. Splunk ties this in easily so you can quickly identify all the users that should have access to certain data but not other types of data, based on their group within a company. Those

types of enterprise features are out of the box in Splunk much more often than in Elastic. Elastic would require more customization and having to build it yourself."

- "In projects like monitoring, data analytics, and observability, for project managers to whom time and security and features are the biggest issue—but not money—they would choose Splunk. Offshore, however, where resources are inexpensive and where you have time to get everything where you want it to be and where out-of-the-box features are not that important, but upfront costs are, then you would look at Elastic."
- "In observability, one of the key competitors is [Cisco's] AppDynamics. Companies use it when specifically dealing with monitoring applications. I've worked on integrating AppDynamics into Splunk but now Splunk is increasingly getting into their space."
- "Yes, [there is some convergence of different tools] but without the security aspect. Usually, the security team is very segregated from the typical functions of IT monitoring, infrastructure monitoring, or observability. They also usually have their own budget. Security usually has leeway to pick their own tools and these don't necessarily match what everyone else in the company is doing."

> **Where resources are inexpensive and where you have time to get everything where you want it to be and where out-of-the-box features are not that important, but upfront costs are, then you would look at Elastic.**
>
> *Professional services consultant for a Splunk partner*

- "It would be difficult to force all these things to converge into a single use case. You can do it in Splunk and we have customers that use Splunk for all these things. But we are not trying to build an all-in-one offering. It wouldn't make sense to reduce the flexibility of clients to decide which parts of Splunk and which premium add-ons they want to buy and how they want to leverage Splunk."
- "[A unified backend] is also the case with Splunk, so it's not a differentiator for Elastic."

Oct. 30, 2020, Splunk report summary: Splunk's move to the cloud is bound to increase its appeal to customers because so many are moving operations off premises. Existing customers are likely to spend more with Splunk as its use cases grow. The growth in Splunk projects with new and existing customers prior to the COVID-19 pandemic should resume. Though pricing is one of Splunk's negatives, the value it provides is worth the cost, especially for large companies, which have greater potential to extract value out from data.

Secondary Sources

This secondary source focused on Amazon's latest release of OpenSearch and its implications for the long-running battle between Amazon and Elastic.

July 13 The Register article

Amazon has released version 1.0 of its Elasticsearch fork, OpenSearch. The company said the platform has added test automation, ensured the code is suitable for production use, and is ready for regular updates. Amazon executives at one time had said they had no plans to fork Elasticsearch into their own product but decided to do so after Elastic changed the licensing structure for its platform. A legal dispute between the two over the Elasticsearch name and trademark appears to be close to a resolution, with Amazon saying it plans to rename its forked product.

- "The AWS-sponsored OpenSearch project has released version 1.0 of its Elasticsearch fork, an evolution of its former project Open Distro for Elasticsearch."
- "'OpenSearch is a community-driven, open source search and analytics suite derived from Apache 2.0 licensed Elasticsearch 7.10.2 & Kibana 7.10.2. It consists of a search engine daemon (OpenSearch), a visualization and user interface (OpenSearch Dashboards), and advanced features from Open Distro for Elasticsearch like security, alerting, anomaly detection and more,' said AWS in a post."
- "Tweaks since the beta version include the introduction of ARM64 architecture support on Linux, and several new features."

- "'Now that OpenSearch has added test automation, built infrastructure, made updates to ensure the code is suitable for production use, and thoroughly tested, the project will be able to deliver on a more regular release cadence,' AWS added."
- "OpenSearch has a confusing and colourful history. AWS launched its Elasticsearch service in October 2015, with Werner Vogels, AWS CTO, declaring on Twitter that it was 'a great partnership between elastic and AWS' (tweet since deleted); however, according to Elastic co-founder and CEO Shay Banon, there was no collaboration and Elastic protested at the use of its Elasticsearch trademark."
- "Elasticsearch was originally mostly licensed under Apache 2.0 but Elastic also offered X-Pack or 'Elastic Stack Features,' first as closed source then under its own less open Elastic license."
- "In March 2019, AWS created its own distribution, calling it the Open Distro for Elasticsearch, based on those parts of the product that are Apache 2.0 licensed. AWS VP and software architect Adrian Cockcroft complained that 'since June 2018, we have witnessed significant intermingling of proprietary code into the code base' of Elasticsearch and that this was 'making it very difficult for developers who want to only work on open source to contribute and participate.'"
- However, he added: 'Our intention is not to fork Elasticsearch, and we will be making contributions back to the Apache 2.0-licensed Elasticsearch upstream project.'"
- "Elastic remained unhappy with the use of the Elasticsearch name and in September 2019 commenced a lawsuit against AWS, stating: 'Due to Amazon's misleading use of the ELASTICSEARCH mark, consumers of search and analytics software are, at least, likely to be confused as to whether Elastic sponsors or approves AESS [Amazon Elasticsearch Service] and Open Distro.'"
- "Banon also claimed last year that 'unfortunately, our copyrights and trademarks have been abused and misused' and at the start of 2021 changed the product to be dual-licensed under its own Elastic License 2.0 or the SSPL (Server Side Public License) devised by MongoDB."
- "This had the effect of making it difficult for cloud providers to run the code as a service since they would have to publish all their proprietary code for managing the service. Elastic's move was unpopular with the open-source community, especially those who had contributed code believing it would always be free to use."
- "AWS responded by introducing OpenSearch in April, based on Open Distro but with a new name and this time explicitly a fork 'derived from Elasticsearch 7.10.2.' The company also introduced OpenSearch Dashboards, a fork of Kibana 7.10.2, a visualisation tool for Elasticsearch data. AWS said that 'we plan to rename our existing Amazon Elasticsearch Service to Amazon OpenSearch Service,' though at the time of writing it remains under the old name."
- "Towards the end of last month, lawyers for Elasticsearch and AWS filed a court document suggesting that the litigation may soon be settled. It notes the forks and the plans to rename the Amazon Elasticsearch Service."

Additional research by Eva Cahen and Emily Carr.